Evaluation Warning: The document was created with Spire.Doc for Python.

**BT（ 4.1.9版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | BT |
| 版本 | 4.1.9 |
| 包名 | co.btchain.bt |
| 域名线索 | 2条 |
| URL线索 | 5条 |
| APP图标 |  |
| 分析日期 | 2024年11月26日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | bt.apk |
| 文件大小 | 45.46MB |
| MD5值 | 9f4ec133b442c62cfa1fcc907878a1f8 |
| SHA1值 | c9730d0cd0005bd99e7f288d547bafe40a4243be |
| SHA256值 | ea109b85f1f8073fe6dcf3366f9e9c298bcbe64c5ee0b4085a8c5af5de3f0c08 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | BT |
| 包名 | co.btchain.bt |
| 主活动Activity | co.btchain.bt.MainActivity |
| 安卓版本名称 | 4.1.9 |
| 安卓版本 | 419 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| ns.adobe.com | 没有服务器地理信息.  |
| github.com | IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/expo/expo/tree/main/packages/expo-splash-screen  | expo/modules/splashscreen/singletons/SplashScreen.java  |
| https://github.com/software-mansion/react-native-screens/issues/17  | com/swmansion/rnscreens/ScreenFragment.java  |
| https://github.com/software-mansion/react-native-screens/issues/17  | com/swmansion/rnscreens/ScreenStackFragment.java  |
| http://ns.adobe.com/xap/1.0/  | lib/armeabi-v7a/libstatic-webp.so  |
| http://ns.adobe.com/xap/1.0/  | lib/armeabi-v7a/libnative-imagetranscoder.so  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=US, ST=Unknown, L=Unknown, O=Unknown, OU=Android, CN=Android Debug 签名算法: rsassa\_pkcs1v15 有效期自: 2013-12-31 22:35:04+00:00 有效期至: 2052-04-30 22:35:04+00:00 发行人: C=US, ST=Unknown, L=Unknown, O=Unknown, OU=Android, CN=Android Debug 序列号: 0x232eae62 哈希算法: sha1 md5值: 20f46148b72d8e5e5ca23d37a4f41490 sha1值: 5e8f16062ea3cd2c4a0d547876baa6f38cabf625 sha256值: fac61745dc0903786fb9ede62a962b399f7348f0bb6f899b8332667591033b9c sha512值: 926c0550edaee7aed1211b91fde06be4cc4748e61d8f1afbe0bd12f3949a0d09a1cf4306c72e6662ae4c7b8ae7a573a81d7e52e5b6124444eaf8f413e6b1fa69 公钥算法: rsa 密钥长度: 2048 指纹: b759a55bdc298b16f7a102f3107f3db38110f3dc7da00b1e981e9b257a9cf1af**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 此APP的危险动作**

| 向手机申请的权限 | 是否危险 | 类型  | 详细情况 |
| --- | --- | --- | --- |
| android.permission.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.READ\_EXTERNAL\_STORAGE | 危险 | 读取外部存储器内容 | 允许应用程序从外部存储读取 |
| android.permission.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.WRITE\_EXTERNAL\_STORAGE | 危险 | 读取/修改/删除外部存储内容 | 允许应用程序写入外部存储 |
| android.permission.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| android.permission.USE\_FINGERPRINT | 正常 | allow use of指纹 | 该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE\_BIOMETRIC |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| co.btchain.bt.MainActivity | **Schemes**: myapp://, co.btchain.bt://,  |

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**